Security Architecture and Design Documentation Guidance

SECURITY REQUIREMENTS

Version 1.1

Prepared by HR CDS TT

23 June 2011

REVISION HISTORY

Name	Date	Reason For Changes	Version
HR CDS TT	19 April 2011	Initial Draft	1.0
HR CDS TT	23 June 2011	Update by the Tiger Team	1.1

ACRONYMS AND DEFINITIONS

Acronym	Definition
CCA	Covert Channel Analysis
CDS	Cross Domain Solution
DRD	Development Representation Documentation
DTLS	Descriptive Top-Level Specification
FTLS	Formal Top-Level Specification
HLD	High Level Design
LLD	Low Level Design
SFS	Security Functional Specification
SP	Security Policy

INTRODUCTION

Security requirements are a clear, unambiguous, and well-defined description of the expected security behavior of the system. This document provides guidance on the development and representation of the system security requirements.

The security requirements are affected by the security architecture and derived from the security objectives and security policy. Figure 1 shows the relationship of the Security Requirements to the other topic areas described in the DRD.

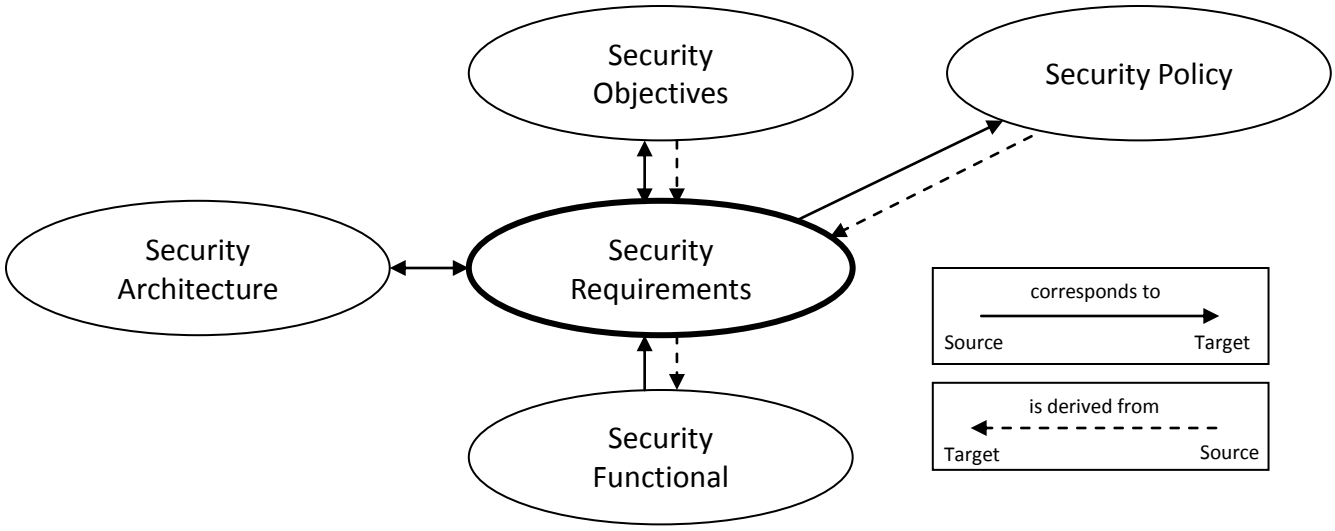

Figure 1 - Security Requirements Interactions

DISCUSSION

Security requirements levied on a system are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

REQUIREMENTS

SRD - 1 The system security requirements shall be stated. The requirements shall:

a. Be clearly and unambiguously expressed.

b. Be internally consistent to enable the development of a system that will meet its security objectives.

c. Be measurable and state objective evaluation requirements such that compliance or noncompliance of a system can be determined and systematically demonstrated.

d. Identify dependencies among security requirements.

SRD - 2 The rationale for the security requirements shall be stated.The rationale shall:

a. Describe why the security requirements satisfy the security objectives and security policy.

b. Demonstrate[1] that the set of security requirements are mutually supportive and internally consistent.

c. Demonstrate that the minimum strength of function level together with any explicit strength of function claim is consistent with the relevant security objectives for the system.

d. Demonstrate that dependent security requirements are satisfied. If any dependencies are not satisfied, then justification shall be provided.

SRD - 3 In order to provide consistency of language in specifiying security requirements, it is recommended that the security functional requirements be drawn from the latest version of the Common Criteria.

SRD - 4 The requirements shall, if appropriate, identify any security requirements for the environment.

[1] Provide a conclusion gained by an analysis which is less rigorous than a "proof".